Anforderungen für „Sichere elektronische Identitäten im Internet“

Einleitung

Das Internet durchzieht heutzutage fast alle Bereiche des täglichen Lebens. Wir führen unsere Bankkonten online, kaufen online ein, verlagern einen Teil des sozialen Lebens in Foren und soziale Netzwerke. Wichtige Grundlage des Handelns im Netz ist das digitale Ich, unsere elektronische Identität im Internet. Sichere elektronische Identitäten sind der Schlüssel für verlässliches und vertrauenswürdiges Handeln im Internet. Jeder Einzelne dürfte mittlerweile über eine Vielzahl elektronischer Identitäten verfügen, mit steigender Tendenz. Bei all diesen Anbietern elektronischer Identitäten existiert in der Regel ein Benutzerkonto mit Benutzername und Kennwort, an welches oft auch persönliche Daten wie Bestellungen, Zahlungen usw. gekoppelt sind.

Mit der zunehmenden Bedeutung unserer elektronischen Identitäten steigt auch das mit einem Verlust und etwaigem Missbrauch verbundene Gefahrenpotential in (Abhängigkeit von den jeweiligen technischen Infrastrukturen). Im Vergleich zum realen Leben mangelt es beim Gebrauch unserer elektronischen Identitäten im virtuellen Raum an allgemein akzeptierten und einfach handhabbaren Mindeststandards, die zu einer gewissen Üblichkeit beim Umgang mit elektronischen Identitäten führen können. Angesichts der häufigen Fälle von Identitätsdiebstahl in letzter Zeit ist eine Überforderung der Nutzer zu befürchten.

Mindeststandards

Sichere elektronische Identitäten sollen branchenübergreifend für alle relevanten Anbieter im Internet „üblich“ werden. Die Nutzerinnen und Nutzer von Internetdienstleistungen sollen einfach erkennen können, dass eine sichere elektronische Identität vorliegt.

Die Mitglieder der AG 4 „Vertrauen, Datenschutz und Sicherheit im Internet“ des IT-Gipfels haben hierzu Mindeststandards für die Anbieter elektronischer Identitäten (Identitätsprovider) formuliert.

Die vorliegenden Mindeststandards werden zunächst von den in der AG 4 vertretenen Identitätsprovidern umgesetzt. Angestrebt wird auch eine Verankerung der Mindeststandards in Kodices, die Dienste betreffen, die elektronische Identitäten voraussetzen.

Binnen eines Zeitraums von zwei Jahren wird überprüft, welche dieser Standards in der Praxis umgesetzt worden sind, von den Nutzern akzeptiert wurden und tatsächlich beitragen, das Schutzniveau nachhaltig zu erhöhen. In die Prüfung ist eine vergleichende Einordnung in den Kontext international bewährter Praktiken („best practices“) vorzunehmen. In Abhängigkeit dieser Evaluation wird eine Selbstverpflichtung der Unternehmerwirtschaft angestrebt. Über den Maßnahmenkatalog und den Umsetzungsstand soll sowohl national als auch international eine breite Transparenz mit dem Ziel einer möglichst flächendeckenden Anwendung hergestellt werden.

Über Mindeststandards hinaus bleibt es Identitätsprovidern weiterhin unbenommen, zusätzliche Möglichkeiten zur Verwendung sicherer elektronischer Identitäten zum Einsatz zu bringen. Sie können und sollen je nach Risikoprofil zusätzlich zum Einsatz kommen.

Maßnahmen

Hinsichtlich der zu ergreifenden technischen Maßnahmen wurde auf technikoffene Beschreibungen Wert gelegt. Bei einigen Maßnahmen ist deren genaue Ausgestaltung hinsichtlich der Identitätsprovider auszudifferenzieren.

Freiwilligkeit

Im Zentrum aller Überlegungen stehen der Nutzer und seine Sicherheit. Bestimmte Sicherheitsmaßnahmen können auch optional angeboten werden. Der Nutzer muss die Möglichkeit haben, sich bewusst gegen eine Nutzung entscheiden zu können (etwa Einsatz eines Sicherheitsschlüssels etc.) bzw. sich bei mehreren Alternativen für eine bestimmte entscheiden zu dürfen (etwa Benachrichtigung per E-Mail).

1. Geeignete Verschlüsselung

Beim Anlegen der Identität, dem Login sowie bei der Nutzung ab Login für relevante Aktivitäten soll eine geeignete Verschlüsselung verwendet werden (z. B. SSL-Verschlüsselung oder Nachfolgestandard).

2. Identifikationsprüfung bei Anlegen der Identität

Ist aufgrund der Art des Angebots eine bestätigte Identität des Kunden erforderlich, sind geeignete Methoden für eine Verifikation der Identität zu wählen.

Standard: Plausibilitätsprüfung oder postalische Anmeldebestätigung.

Add-On: Online-Ausweisfunktion des neuen Personalausweises, PostIdent.

3. Mindestanforderungen zur Passwortsicherheit

Anforderung an sicheres Passwort sollen anbieterseitig eingefordert werden. Eine Speicherung der Passwörter beim Anbieter soll verschlüsselt / gehasht erfolgen.

Standard: Speicherung des Passworts nur als Hash in Datenbank.

Add-On: Speicherung des Passworts als Hash und „salted“ (zusätzlich verfälscht)

4. Regelmäßige Informationspflichten über relevante Aktivitäten im Account, z. B. Anzeige des letzten Logins

Dient der Information des Kunden und trägt zur Transparenz bei.

Standard: Anzeige bei Login oder in bestimmtem Bereich.

Add-On: Information auf unabhängigem Kanal (z. B. E-Mail, SMS, De-Mail).

5. Besondere Transaktionssicherung

Je nach Risikoprofil einer Transaktion mit besonderem Sicherheitsbedarf sind entsprechende Sicherungsmaßnahmen erforderlich

Standard: Je nach Sicherheitsbedarf mobileTAN oder Hardware-Token, sichere Zahlungssysteme.

Add-On: Online-Ausweisfunktion des neuen Personalausweises zuzüglich Absicherung der Verbindung.

6. Deutlich sichtbarer Logout-Button

Auf allen Seiten des Internetauftritts soll der Logout-Button sichtbar sein.

Standard: Deutlich sichtbar auf allen Seiten.

Add-On: Automatischer Logout nach Inaktivitätszeit.

7. Informationspflicht des Anbieters bei mutmaßlichem Verlust der Identität

Information des Nutzers bei Kenntniserlangung (z. B.: Unregelmäßigkeiten bei der Nutzung, Anzeige Dritter, Einbruch in die Kundendatenbank).

Standard: Information per E-Mail, SMS.

Add-On: Information per DE-Mail, Brief oder vergleichbare Alternative.

8. Pflicht zur Sperrung des Accounts bei Verlust der Identität

Pflicht des Identitätsproviders ab Anzeige durch Kunden oder sonstiger gesicherter Kenntniserlangung.

9. Einfache Mitnahmemöglichkeit des Account-Inhalts (Exportfunktion)

Sichere elektronische Identitäten sind eng verknüpft mit der Wahlfreiheit des Nutzers für einen Providerwechsel oder eine unproblematische Kündigung des Accounts. Hinterlegte Daten (Adressbücher, Medieninhalte etc.) des Kunden sollen daher in einem gängigen Format transferiert werden können (wenn nach Art des Angebots möglich und sinnvoll). Anbieterbezogene Kundenkennungen (name@provider.tld) sind von der Mitnahmemöglichkeit ausgeschlossen.

10. Löschungspflicht nach Kündigung des Accounts

Die Kündigung eines Accounts muss einfach möglich sein. Dabei muss für den Kunden sichergestellt sein, dass auch die über ihn gespeicherten Daten (Profil) – ggf. nach einer Übergangszeit von max. 3 Monaten und abhängig von gesetzlichen Aufbewahrungspflichten – gelöscht werden.

AG 4-Mitglieder

- 1&1 Internet AG
- BITKOM e. V.
- Bundesamt für Sicherheit in der Informationstechnik
- Bundesbeauftragter für den Datenschutz
- Bundesministerium des Innern
- Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz
- Bundesverband Deutscher Banken e. V.
- Deutsche Post AG
- Deutsche Telekom AG
- Deutschland sicher im Netz e. V.
- eBay GmbH
- eco – Verband der deutschen Internetwirtschaft e. V.
- Fraunhofer SIT
- Giesecke & Devrient GmbH
- Hewlett-Packard GmbH
- LVM Versicherung
- Microsoft Deutschland GmbH
- secunet Security Networks AG
- Verbraucherzentrale Bundesverband e. V.
- Vodafone D2 GmbH
- VZ Netzwerke Ltd