Die digitale Souveränität:

Die Authentifizierung als bestimmendes Element eines digitalen Prozesses

Betrachtung

Inhaltsverzeichnis

1 Die digitale Souveränität

Wird über digitale Souveränität gesprochen, stehen viele Aspekte zur Diskussion.
Verschiedene Institutionen bieten hierfür ausführliche Informationen und auch Definitionen an.

1.1 Definitionen

Nachfolgend einige Definitionen:

„Digitale Souveränität ist die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.“ [1]

„Wir bewahren die Fähigkeit zu autonomem Handeln. Bei Schlüsseltechnologien, Diensten und Plattformen verfügen wir über Fähigkeiten auf dem neuesten Stand der Technik. Wir können frei und verantwortungsbewusst zwischen eigenen Lösungen und tragfähigen Optionen vertrauenswürdiger globaler Partner wählen.“ [2]

1.2 Unser Verständnis

Für uns bedeutet digitale Souveränität die **Vermeidung digitaler Abhängigkeiten** und **die Kontrolle wesentlicher digitaler Prozesse**.
Da wir eine praktische Umsetzung in Lösungen anstreben, gilt unser Fokus in dieser Betrachtung einem besonderen, aber wesentlichen Aspekt der Digitalisierung:
Der Authentifizierung, also der Verifizierung einer digitalen Identität.

[1] https://www.oeffentliche-it.de
[2] https://www.bitkom.org

2 Die Authentifizierung: Der Beginn nahezu jedes digitalen Prozesses

Nahezu täglich, im Home-Office oder im Büro, starten wir unseren PC.

Der erste Vorgang überhaupt ist die Authentifizierung, also die Anmeldung am System. Dazu werden üblicherweise ein Benutzer-Kennwort und Passwort verwendet. Stimmen diese mit dem im System hinterlegten Daten überein, dann wird der Zugang zum System gewährt.
Dieser Vorgang soll unabhängig davon betrachtet werden, ob die Authentifizierung auf dem PC oder über einen Verzeichnisdienst über das Netzwerk erfolgt.

Doch wer verwaltet eigentlich diese Zugangsdaten?

Das Betriebssystem verwaltet diese Daten auf mehr oder weniger transparente Weise.
Als Anwender können wir die vom Betriebssystem zur Verfügung gestellten Werkzeuge nutzen, um Benutzer-Konten zu verwalten. Der Benutzer selbst kann ebenfalls über Werkzeuge des Betriebssystems sein Passwort verwalten. Dadurch kann niemand innerhalb einer Organisation das Passwort entschlüsseln.

Aber wer hat die Kontrolle darüber?

Das Benutzer-Kennwort und das Passwort werden bei der Benutzer-Anmeldung im Klartext eingegeben. Also erhält das Betriebssystem, und dadurch indirekt auch der Betriebssystem-Hersteller diese Daten.

Natürlich gehen wir davon aus, dass der Hersteller mit den Anmeldedaten korrekt umgeht.
Aber aus technischer Sicht wäre es möglich, diese Daten an einen anderen Server außerhalb des eigenen Netzwerkes zu übertragen, wenn der Rechner z.B. mit dem Internet verbunden wäre.

Dasselbe gilt natürlich nicht nur für Desktop-Betriebssysteme, sondern auch für alle Arten von Web-Diensten.

3 Die Optionen

Es stehen verschiedene Optionen zur Verfügung, um mehr Kontrolle über die Authentifizierung zu erlangen.

3.1 2-Faktor-Authentifizierung

Um Zugänge zu schützen, wird oft eine 2-Faktor Authentifizierung verwendet. Diese benötigt zur Freischaltung einen weiteren Faktor wie z.B. einen Pin.
Im angesprochenen Fall würde diese Vorgehensweise aber keinen Vorteil bringen, da der 2. Faktor ja im System hinterlegt wäre.

3.2 Authentifizierung ohne Passwort

Die einzige Lösung, die einen Missbrauch der Anmeldedaten verhindern könnte, wäre eine Authentifizierung ohne Passwort. Wird kein Passwort verwendet, kann dieses auch nicht missbraucht werden.
Es gibt mittlerweile verschiedene Möglichkeiten einer Authentifizierung ohne Passwort.

3.2.1 Authentifizierung über Smartcards

Die Authentifizierung über Smartcards ist sowohl am Windows Desktop als auch am Remote Desktop möglich. Aktuell gibt es aber keinen Standard bzw. Implementierungen für Web-Anwendungen oder mobile Geräte. Dazu wird eine Smartcard benötigt, die mit entsprechenden Schlüsseln versehen werden muss.

3.2.2 Authentifizierung über moderne Protokolle

Seit einiger Zeit unterstützten auch Standard-Betriebssysteme z.B. die Authentifizierung über das FIDO2-Protokoll. Dies gilt sowohl für die lokale Anmeldung als auch über Verzeichnisdienste. Es gibt auch Implementierungen für nahezu alle Browser, sodass diese Option auch für Web- Anwendungen geeignet ist. Mobile Geräte werden ebenfalls unterstützt.
Allerdings wird hier i.d.R. ein Hardware-Token z.B. mit USB-Schnittstelle sowie eine einmalige Registrierung benötigt. Der Benutzer kann seinen Pin über entsprechende Tools des Token-Herstellers bestimmen.

4 Unsere Lösung

Als Beginn nahezu jeden digitalen Prozesses kommt der Authentifizierung eine hohe Bedeutung zu. Wenn digitale Souveränität die Kontrolle über wesentliche digitale Prozesse bedeutet, dann ist es unumgänglich, die Kontrolle über die Authentifizierung zu haben.
Diese ist aktuell nur bedingt gegeben.

4.1 Authentifizierung über den digitalen Personalausweis

Der digitale Personalausweis ist bereits seit einigen Jahren verfügbar, wird aber bisher hauptsächlich für die Identifizierung eingesetzt. Laut Schätzungen sollen 2021 über 40 Millionen Ausweise mit aktivierter Online-Ausweisfunktion existieren.
Sieht man jedoch die Authentifizierung als eine Art „Identifizierung light“ an, so können verfügbare Möglichkeiten einfach genutzt werden.

Warum der digitale Personalausweis?

Dafür gibt es mehrere Gründe:

Elektronischer Personalausweis	Alternative-Systeme
Der ePerso kann für die Authentifizierung UND Identifizierung eingesetzt werden.	Die alternativen Systeme sind ausschließlich für Authentifizierung ausgelegt.
Hinter dem ePerso steht die Autorität eines Staates.	Hinter den o.g. Systemen stehen Wirtschaftsunternehmen aus dem Ausland.
Der ePerso benötigt für eine Organisation einen geringen Verwaltungsaufwand.	Der Verwaltungsaufwand bei der Konfiguration des Tokens ist weitaus höher.
Bei Verlust des ePerso gibt es eine 24/7 Sperr-Hotline.	Im Falle eines Tokens ist das Unternehmen i.d.R. zu Betriebszeiten dafür verantwortlich.
Der ePerso garantiert höchstmögliche Sicherheit durch entsprechende Zertifikate, welche aktuell nur eine Instanz ausstellen kann.	Die Zertifikate werden vom Unternehmen selbst verwaltet.
Die Kosten liegen auf vergleichbarem Niveau.	

5 Zusammenfassung

Soll ein Minimum an digitaler Souveränität erreicht werden, so ist die Kontrolle über die Authentifizierung notwendig.
Ist diese Kontrolle gegeben, ist damit auch ein Höchstmaß an Sicherheit verbunden.
Generell gilt dies für Betriebssysteme als auch für Web-Dienste.

Dazu gibt es eigentlich nur die Alternative der passwortlosen Authentifizierung.
Die Optionen dazu wurden genannt.

Der elektronische Personalausweis zählt ebenfalls dazu und stellt durch Ausweis und Pin ein 2-Faktor-System dar. In naher Zukunft sollte eine flächendeckende Verbreitung erreicht sein.

Die Autorität eines Staates und die damit verbundene Unabhängigkeit und Sicherheit haben den Ausschlag gegeben, eine Implementierung der Authentifizierung über den elektronischen Personalausweis in unsere Lösung durchzuführen.

Dadurch möchten wir unseren Beitrag für mehr digitale Souveränität leisten.