Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Informatiksteuerungsorgan Bund ISB
Informatiksicherheit SEC

Rolf Oppliger, ISB
Daniel Markwalder, BIT
François Weissbaum, FUB

29. Juni 2012

Technologiebetrachtung

Passwörter vs. PINs

1 Einleitung

Seit 2004 unterliegen die in der Bundesverwaltung eingesetzten Passwörter der Anforderung 2.4 des Anhangs 1 der Weisungen über die Informatiksicherheit in der Bundesverwaltung (WIsB). Unter anderem müssen Passwörter mindestens 8 Zeichen lang sein[1], Gross- und Kleinbuschstaben, Ziffern und Sonderzeichen enthalten und nach 5 Fehlversuchen bei der Eingabe gesperrt werden.

Unabhängig von diesen Vorgaben sind verschiedene Hardware-Token und Geräte mit persönlichen Identifikationsnummern (PINs) konfiguriert, um einen gewissen Schutz vor Verlust und Missbrauch zu erwirken. Die Idee ist, dass ein solches Token oder Gerät nur durch Eingabe einer PIN freigeschalten und genutzt werden kann. Solche PINs kommen insbesondere bei Smartcards und Smartphones zum Einsatz. Jemand der ein so geschütztes Token oder Gerät findet oder absichtlich entwendet, kann dieses nur nutzen, wenn er auch die korrekte PIN kennt und über eine Tastatur eingeben kann. Üblicherweise ist dabei die Anzahl Versuche dahingehend begrenzt, dass die Benutzerin oder der Benutzer nur eine bestimmte Anzahl von Versuchen hat, um die korrekte PIN einzugeben. Gelingt dies nicht wird das Token oder Gerät gesperrt. Ob und wie eine Entsperrung erfolgen kann, hängt insbesondere vom Token oder Geräte ab.

Weil Passwörter und PINs über bestimmten Alphabeten gebildete Zeichenketten darstellen, sehen sie für die Benutzerin und den Benutzer (syntaktisch und semantisch) gleich aus. Entsprechend drängt sich die Frage auf, ob PINs auch unter die Passwortbezogenen Vorgaben der WIsB fallen. Das hätte natürlich auch Auswirkungen auf die Art und Weise, wie PINs ausgewählt werden können und wie sie allenfalls zu handhaben sind. Ziel dieser Technologiebetrachtung ist es, bis zur Inkraftsetzung der überarbeiteten WIsB in diesen Fragen Klarheit zu schaffen.

[1] Für Administratorenpassworte gilt eine Minimallänge von 12 Zeichen.

2 Konzeptionelle Unterschiede

Wie bereits erwähnt sehen Passwörter und PINs für die Benutzerinnen und Benutzer gleich aus. Nichtsdestotrotz gibt es eine Reihe von konzeptionellen Unterschieden, die eine unterschiedliche Handhabung und damit auch unterschiedliche Sicherheitsvorgaben rechtfertigen:

1. Im Gegensatz zu einem Passwort ist eine PIN an ein Token oder Gerät gebunden, das - im Rahmen einer Zwei-Faktoren-Authentifikation - einen zweiten Faktor darstellt. Mit einer PIN alleine kann ein Angreifer nichts anfangen, d.h. er muss noch in den physischen Besitz des jeweiligen Tokens oder Gerätes gelangen. Damit ist ein PIN im Vergleich zu einem Passwort weniger kritisch.
2. Passwörter und PINs sind unterschiedlichen Angriffsszenarien ausgesetzt: Während bei einem Passwort Offline-Wörterbuchangriffe[2] immer möglich sind und die hauptsächlichen Sicherheitsrisiken beim Einsatz darstellen, ist bei einer PIN nur ein Online-Angriff möglich. Bei einem solchen Angriff muss die Überprüfung der PIN zwingend auf dem Token oder Gerät erfolgen. Dies bedeutet einerseits, dass der Angreifer physisch im Besitz des Tokens oder Gerätes sein muss, und andererseits, dass die Anzahl Versuche, die ein Angreifer maximal tätigen kann, effektiv kontrolliert und begrenzt werden kann. Das macht aus sicherheitstechnischer Sicht einen grossen Unterschied.
3. Während Passwörter meist über normale Tastaturen eingegeben werden, erfordert die Eingabe einer PIN meist eine dedizierte und in Bezug auf den zur Verfügung stehenden Zeichensatz beschränkte Tastatur. Im Falle von qualifizierten Signaturen sollten aus Sicherheitsgründen z.B. Kartenleser der Klasse 2 oder höher eingesetzt werden. Solche Kartenleser verfügen meist nur über ein numerisches Tastaturfeld, d.h. die Eingabe von Buchstaben ist hier technisch nicht möglich. Entsprechend hat es keinen Sinn, hier z.B. ein aus Klein- und Grossbuchstaben und Sonderzeichen bestehendes Alphabet zu verlangen.

3 Schlussfolgerungen

Aufgrund der obigen Ausführungen stellt eine PIN kein Passwort dar und fällt entsprechend auch nicht unter die Passwort-bezogenen Anforderungen der WIsB. In der sich zur Zeit in Überarbeitung befindlichen WIsB werden Anforderungen an PINs noch spezifiziert. Diese hängen auch von den damit zu schützenden Token und Geräten bzw. von allfälligen technischen Restriktionen ab. Für den Fall von PINs für Smartcards verlangt das VBS, dass eine PIN aus einem mindestens die Ziffern 0 – 9 umfassenden Alphabet gebildet ist , mindestens die Länge 6 hat und bei der Eingabe höchstens 5 Versuche zugelassen sind[3]. Dabei handelt es sich um Minimalanforderungen, d.h. aus sicherheitstechnischer Sicht kann man immer empfehlen, so-

---

[2] Bei einem Offline-Wörterbuchangriff verfügt der Angreifer über Bilder von Passwörtern, die mit einer Einweg-Funktion (z.B. kryptografische Hashfunktion) erstellt worden sind. Diese können einer Datenbank entnommen oder während ihrer Übertragung in einem Computernetz abgegriffen worden sein. Der Angreifer kann dann unter Zuhilfenahme beliebiger Rechenleistung beliebige Wörter unter der Einweg-Funktion abbilden und auf Übereinstimmung prüfen. Im positiven Fall hat der Angreifer ein gültiges Passwort gefunden.

[3] Mathematisch gesehen hat die Anzahl Versuche nur einen marginalen Einfluss auf die Sicherheit. Bei einer numerischen PIN der Länge 6 hat ein Angreifer bei maximal 3 Versuchen z.B. eine Erfolgswahrscheinlichkeit von $3/10^6 = 0.000003$, während er bei maximal 5 Versuchen eine Erfolgswahrscheinlichkeit von $5/10^6 = 0.000005$ hat. Beide Werte sind für den praktischen Einsatz hinreichend klein.

wohl das Alphabet und die Länge der PIN zu vergrössern als auch die Anzahl möglicher Versuche bei der Eingabe zu verkleinern. Ob und wie stark das allerdings möglich ist, muss im Einzelfall abgeklärt werden.

Wichtiger als das Alphabet, die Länge und die Anzahl Versuche bei der Eingabe einer PIN ist in jedem Fall die Anforderung, dass eine PIN nicht trivial ist (z.B. „123456“) und nicht einem für die Besitzerin oder den Besitzer persönlichen Wert (z.B. Geburts- oder Hochzeitstag) entspricht bzw. davon abgeleitet werden kann. Während ersteres allenfalls noch proaktiv getestet werden kann, ist man bei zweiterem auf die Mitwirkung der Besitzerin oder des Besitzers angewiesen. Entsprechend kommt der Sensibilisierung und Schulung der Mitarbeitenden in diesem Zusammenhang eine grosse Bedeutung zu.

Abkürzungen

BIT	Bundesamt für Informatik und Telekommunikation
EFD	Eidgenössisches Finanzdepartement
FUB	Führungsunterstützungsbasis
ISB	Informatiksteuerungsorgan Bund
PIN	Persönliche Identifikationsnummer
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
WIsB	Weisungen über die Informatiksicherheit in der Bundesverwaltung