Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Informatiksteuerungsorgan Bund ISB
Informatiksicherheit SEC

Rolf Oppliger

22. August 2016
(revidiert am 5. Dezember 2016)

Technologiebetrachtung

Ist die Erzwingung eines periodischen Passwortwechsels sinnvoll?

1 Einleitung

Gemäss Anforderung 7.1.2 des IKT-Grundschutzes [1] müssen „mittels Passwort[1] geschützte IKT-Mittel einen automatischen, periodischen Passwortwechsel erzwingen. Ist dies technisch nicht machbar, müssen die Benutzer in geeigneter Weise auf das regelmässige Ändern des Passworts aufmerksam gemacht werden." In Anforderung 8.1 wird zudem die maximale Gültigkeit eines Passwortes auf 90 Tage beschränkt. Beiden Anforderungen liegt die Annahme zugrunde, dass durch einen periodischen Passwortwechsel die Verwundbarkeit eines IKT-Systems oder einer Anwendung zeitlich verringert und die Sicherheit damit erhöht werden kann. Diese Annahme stammt aus den Anfangszeiten der IKT, als das Ausprobieren aller möglichen Passwörter für einen Angreifer noch aufwändig war und entsprechend lange Zeit in Anspruch nahm. Obwohl die Situation heute anders ist und die Annahme kritisch hinterfragt werden muss, ist die Erzwingung eines periodischen Passwortwechsels in vielen Vorgaben für die IKT-Sicherheit und den sicheren Umgang mit Passwörtern immer noch enthalten (so z.B. auch in [1]). Weil Benutzer immer mehr Passwörter haben und diese zum Teil auch synchron halten müssen, wird die Einhaltung dieser Vorgabe aus Benutzersicht zunehmend schwierig.

Vor diesem Hintergrund stellt sich die Frage, ob bzw. wie sinnvoll die Erzwingung eines periodischen Passwortwechsels wirklich ist, bzw. ob die oben erwähnten Anforderungen des IKT-Grundschutzes nicht grundsätzlich überdacht und angepasst werden müssen. Diese Frage und deren Beantwortung stehen im Mittelpunkt dieser Technologiebetrachtung.

[1] Man beachte, dass diese Anforderung nur für Passwörter und nicht für PINs im Sinne von [2] gilt.

2 Wissenschaftliche Untersuchungen und Schlussfolgerungen

Für die Erzwingung eines periodischen Passwortwechsels spricht zunächst einmal das Argument, dass damit das Verwundbarkeitsfenster für die Ausnutzung eines kompromittierten Passwortes zeitlich begrenzt werden kann. Ohne diesen Mechanismus ist ein kompromittiertes Passwort solange nutzbar, wie der Benutzer sein Passwort nicht ändert. Das kann im Extremfall immer sein, so dass ein kompromittiertes Passwort so lange nutzbar ist wie das Benutzerkonto existiert. Weil Benutzerkennungen und Passwörter im Internet über lange Zeitspannen gehandelt werden, stellen kompromittierte Passwörter ein Problem dar, das mit der Erzwingung eines periodischen Passwortwechsels in seinen Auswirkungen reduziert werden kann. Wie stark die Reduktion aber wirklich ist, ist a priori nicht klar. Es gibt mindestens zwei Argumente, wonach die Erzwingung eines periodischen Passwortwechsels das Problem nicht wesentlich reduziert: Auf der einen Seite wird ein Angreifer mit seinem Angriff nicht warten, bis der Benutzer sein Passwort gewechselt hat, d.h. der Angriff wird zeitnah und unmittelbar nach der Kompromittierung stattfinden. Ein allenfalls später erzwungener Passwortwechsel bietet dann keinen Schutz. Auf der anderen Seite ist es in vielen Angriffsszenarien nicht einmal erforderlich, dass der Angreifer ein Passwort im Klartext kennt. Man denke hier etwa an „Pass-the-Hash“-Angriffe, wie sie z.B. in [3] beschrieben sind.

Die Frage, ob bzw. wie sinnvoll die Erzwingung eines periodischen Passwortwechsels aus heutiger Sicht wirklich ist, ist in der jüngeren Vergangenheit im Mittelpunkt von mindestens zwei wissenschaftlichen Untersuchungen gestanden.

- In [4] ist mit Hilfe empirischer Untersuchungen gezeigt worden, dass ein Angreifer, der ein Passwort eines Benutzers kennt, in vielen Fällen auf ein neues Passwort schliessen kann, wenn dieser Benutzer zu einem Passwortwechsel gezwungen wird.
- In [5] ist zudem quantitativ gezeigt worden, dass es für einen Angreifer nicht viel schwieriger ist, ein gültiges Passwort zu finden, selbst wenn dieses Passwort während der Suche – z.B. aufgrund eines erzwungenen Passwortwechsels – geändert wird.

Beide Untersuchungen zeigen auf, dass der Sicherheitsgewinn eines erzwungenen Passwortwechsels nicht allzu gross ist, und dass die Erzwingung eines periodischen Passwortwechsels deshalb relativiert und in Frage gestellt werden kann.

3 Einschätzung

Aufgrund der obigen Ausführungen kann der sicherheitstechnische Nutzen der Erzwingung eines periodischen Passwortwechsels als fragwürdig eingestuft werden. Demgegenüber stehen hohe Aufwände bzw. Kosten bei der Passwortverwaltung. Insbesondere auf der Seite der Benutzer wird es zunehmend schwierig, Passwörter mit unterschiedlichen Laufzeiten zu unterschiedlichen Zeitpunkten auszuwechseln und synchron zu halten. Einem relativ geringen und konstanten Nutzen stehen damit nicht unerhebliche und stetig steigende Kosten gegenüber. Es ist deshalb wohl nur eine Frage der Zeit, bis die Kosten den Nutzen übersteigen.

Vor diesem Hintergrund haben ein paar Sicherheitsbehörden ihre einschlägigen Empfehlungen angepasst. So empfiehlt z.B. die britische Communications Electronics

Security Group (CESG[2]) von der Erzwingung eines periodischen Passwortwechsels explizit abzusehen [6], während das U.S. amerikanische National Institute of Standards and Technology (NIST) eine differenzierte Betrachtungsweise vorschlägt [7]. Demnach haben unterschiedliche Systeme und Anwendungen auch unterschiedliche Anforderungen betreffend der Erzwingung eines periodischen Passwortwechsels. Gegen einen erzwungenen Passwortwechsel haben sich zuletzt auch die Cheftechnologin[3] der U.S. amerikanischen Federal Trade Commission (FTC) und namhafte IKT-Anbieter ausgesprochen[4]. So hat z.B. Microsoft in soeben erschienenen Empfehlungen zum Einsatz von Passwörtern [8] das zeitliche Auslaufen von Passwörtern und das damit verbundene Erzwingung von periodischen Passwortwechseln als „Anti-Pattern“ aufgeführt, d.h. als Ansatz, der zwar verbreitet ist, insgesamt aber eher negative Auswirkungen auf die IKT-Sicherheit hat.

Das ISB geht mit der CESG einig, dass ein periodischer Passwortwechsel nicht in jedem Fall erzwungen werden soll, bzw. mit dem U.S. amerikanischen NIST, wonach es im Einzelfall auch auf die Systeme und Anwendungen ankommt. Während es für besonders kritische Systeme und Anwendungen durchaus Sinn machen kann, einen periodischen Passwortwechsel zu erzwingen, trifft das für alle anderen nicht zu. Dann macht es aber auch keinen Sinn, eine solche Anforderung im IKT-Grundschutz zu belassen.

In einer Analogie mit der physischen Welt könnte man einen Passwortschutz mit einem Türschloss vergleichen. Niemandem käme es ernsthaft in den Sinn, aus prophylaktischen Gründen Türschlösser periodisch zu ersetzen. Solche Schlösser werden erst dann ersetzt, wenn ein Schlüssel verloren gegangen ist oder es einen konkreten Verdacht gibt, dass ein Schlüssel hätte kopiert werden können. Ähnliches gilt auch für Passwörter in der digitalen Welt: Diese werden sinnvollerweise nur dann ersetzt bzw. gewechselt, wenn sie kompromittiert worden sind oder es einen Verdacht auf eine Kompromittierung gibt. Ein prophylaktischer Wechsel ist nicht sinnvoll bzw. mit zu grossen Nachteilen verbunden.

4 Weiteres Vorgehen

Das ISB wird die Erzwingung eines periodischen Passwortwechsels im Sinne von Anforderung 7.1.2 und 8.1 des IKT-Grundschutzes prüfen und je nach Ergebnis die entsprechenden Grundschutzmassnahmen anpassen. Im Sinne der Empfehlung des U.S. amerikanischen NIST wird es im Einzelfall den Verantwortlichen von IKT-Systemen und Anwendungen überlassen sein, einen periodischen Passwortwechsel zu erzwingen, wenn dies sicherheitstechnisch sinnvoll ist (z.B. für Administratorenpasswörter). Werden Passwortwechsel nicht erzwungen, sind geeignete Vorkehrungen zu treffen, damit – mit Hilfe von detektiven Massnahmen – kompromittierte Passwörter möglichst zeitnah erkannt werden können. Solche Vorkehrungen sind unabhängig von einem allfällig erzwungenen Passwortwechsel sowieso sinnvoll. Eine Möglichkeit besteht z.B. darin, dass man einen Benutzer z.B. im Rahmen seiner Login-Maske darüber informiert, wann sein Passwort zuletzt verwendet worden ist. Entsprechend sensibilisierte Benutzer werden dann auch Missbräuche einfacher erkennen und darauf reagieren können.

---

[2] Die CESG ist der Teil der Government Communications Headquarters (GCHQ), der sich mit Informationssicherheit befasst.

[3] Dr. Lorrie Cranor

[4] https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes

Abkürzungen

FTC	Federal Trade Commission
CESG	Communications Electronics Security Group
GCHQ	Government Communications Headquarters
IKT	Informations- und Kommunikationstechnologie
ISB	Informatiksteuerungsorgan des Bundes
NIST	National Institute of Standards and Technology
PIN	Personal Identification Number
U.S.	United States
z.B.	zum Beispiel

Referenzen

[1] ISB, Si001 - IKT-Grundschutz in der Bundesverwaltung, Version 3.0 vom 19.12.2013, https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/sicherheit/si001-ikt-grundschutz_in_der_bundesverwaltung.html

[2] ISB, Technologiebetrachtung Passwörter vs. PINs, 29.6.2012, https://www.isb.admin.ch/dam/isb/de/dokumente/themen/sicherheit/pw-pin.pdf.download.pdf/pw-pin.pdf

[3] ISB, Technologiebetrachtung „Pass-the-Hash"-Angriffe, 19.11.2012, https://www.isb.admin.ch/dam/isb/de/dokumente/themen/sicherheit/PassTheHash.pdf.download.pdf/PassTheHash.pdf

[4] Yinqian Zhang, Fabian Monrose und Michael K. Reiter, The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis, Proc. 17th ACM Conference on Computer and Communication Security (CCS'10), October 2010, pp. 176 – 186, http://cs.unc.edu/~fabian/papers/PasswordExpire.pdf

[5] Sonia Chiasson und Paul C. van Oorschot, Quantifyinfg the Security Advantage of Password Expiration Policies, *Designs, Codes and Cryptography*, Vol. 77, Issue 2-3, December 2015, pp. 401 – 408, http://people.scs.carleton.ca/~paulv/papers/expiration-authorcopy.pdf

[6] Communications Electronics Security Group (CESG), *Password Guidance: Simplifying Your Approach*, 15. März 2016, https://www.cesg.gov.uk/content/files/document_files/Password_guidance_-_simplifying_your_approach_back_cover.pdf

[7] U.S. National Institute of Standards and Technology (NIST), Draft Special Publication (SP) 800-118, *Guide to Enterprise Password Management*, 21. April 2009, http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

[8] Microsoft, Microsoft Password Guidance, 2016, https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf