Produkt DresPleierPwS - Passwörter nicht-digital sicher speichern und verwenden

DresPleier GmbH, 84149 Velden, Deutschland

Passwörter sind sehr wichtig und werden weiterhin viel genutzt. Auch in Varianten als Passwort, PIN, PUK, Passphrase usw. Anwender haben in der Regel viele Passwörter mit unterschiedlicher Kritikalität vom trivialen Internet-Dienst bis zum hochprivilegierten Administrator-Passwort. Sie müssen stark, änderbar und an unterschiedlichen Geräten und Einsatzorten verwendbar sein. Eine Möglichkeit damit umzugehen sind Passwort-Manager-Programme. Diese speichern Passwörter digital und stark gesichert, bieten jedoch entsprechende digitale Angriffsmöglichkeiten bis hin zum Erlangen aller gespeicherter Passwörter. Eine Alternative oder auch Ergänzung hierzu ist die Passwortspeicherung außerhalb der IT-Systeme mit deutlich reduzierten Angriffsrisiko, da diese nicht digital bzw. nicht über das Netz erreichbar sind. Einfach machbar ist dies durch Aufschreiben auf Zetteln mit sicherer Verwahrung. Will man diese jedoch besser schützen oder auch mitnehmen, so ist ein besonderes Sicherheitskonzept gefragt. Dieser Artikel beschreibt das von der DresPleier GmbH entwickelte innovative und sehr pragmatisch nutzbare Konzept DresPleierPwS[1] hierzu.

Motivation

Passwort-Manager-Programme zur kombinierten Speicherung und Nutzung von Passwörtern sind viel im Einsatz. Sie bieten Komfort durch die Speicherung und Verwendung via Zwischenablage oder anderen Methoden und in der Regel ein hohes Sicherheitsniveau durch zahlreiche Schutzmaßnahmen. Sie können jedoch problematisch sein. Denn sie bieten durch die digitale Speicherung in Kombination mit der heutzutage üblichen Vernetzung viele Angriffsmöglichkeiten wie einen Lauschangriff auf das Zugangspasswort, einen unberechtigten Zugriff bzw. Diebstahl der Speicherdatei, insbesondere dann, wenn in der Cloud abgelegt. Die Manager enthalten gebündelt die Passwörter, meist mit Zusatzinformationen zur Anwendung wie zugehörige Zugriffs-URLs und Kennungen der Dienste. Kann ein Angreifer diese Daten bekommen und knacken, hat er umfangreiche Informationen für den Missbrauch. Eine Alternative oder auch in Mischform genutzte Ergänzung sind nicht-digital gespeicherte Passwörter. Ein Zettel mit den Kennungen und Passwörtern, gut geschützt vor Missbrauch verwahrt beispielsweise in einem Tresor, ist eine einfache und sehr sichere Lösung. Die Frage ist jedoch, ob man den Schutz verbessern kann. Dies insbesondere, wenn man Passwörter auch mobil und an unterschiedlichen Orten nutzen möchte oder z.B. auf Reisen keine Schutzmöglichkeit wie ein Tresor zur Verfügung steht. Nachfolgend ein Konzept dazu:

Basiskonzept

Konzeptteil 1: Speichere keine Passwörter gebündelt, also gesammelt digital, insbesondere nicht außerhalb des eigenen Kontrollbereichs, also nicht in der Cloud oder vergleichbaren Web-Storage. Angebote bzw. Dienste, um Passwörter Geräte-/System-übergreifend zu nutzen, indem sie auf Cloud-Speichern gehalten und durch Verschlüsselung geschützt werden, bieten keinen empfehlenswerten Schutz, denn sie ermöglichen Dritten (wie dem Cloud-Storage-Provider) direkten Zugriff auf die Speicherdatei. Auch bei lokaler Speicherung ist Verschlüsselung der typische Schutzmechanismus und gilt als sicher, sofern geeignet stark. Die Erfahrungen der Vergangenheit haben jedoch bewiesen, daß dies nicht immer gesichert so ist, da sie kompromittiert (z.B. Manipulation des Zufallszahlengenerators in Debian) oder fehlprogrammiert (z.B. Heartbleed-Bug) sein kann. Insofern ist es weise, besonders schützenswerte Daten erst gar nicht in fremde Hände gelangen zu lassen. Bei dem Konflikt zwischen Komfort und Sicherheit, der individuell bzw.

1 PwS steht für Passwort-Speicher

gemäß der konkreten Risikolage abzuwägen ist, führt dies bei Gewichtung auf Sicherheit zu **Konzeptteil 2: Speichere Passwörter außerhalb der IT, z.B. in einem Notizbuch, auf einem Zettel, auf einem Bankkarten-großen Plastikobjekt o.ä.**

Passwörter sollen stark sein, dazu lang und komplex, gegebenenfalls sind sie auch zu ändern, z.B. falls sie bekannt wurden. Dies ist zu berücksichtigen, die Notizbuch- oder Zettel-Lösung muss Veränderungen ermöglichen, dies ergibt **Konzeptteil 3: Ermögliche dynamische Änderungen der gespeicherten Passwörter** und kombiniert die Anforderung **Konzeptteil 4: Nutze veränderliche Komponenten, z.B. Bleistift (da radierbar) oder eine Kombination von Papier und Klarsicht-folie, die gemeinsam genutzt werden (z.B. übereinandergelegt)**. Man verwendet also z.B. ein Blatt Papier in Bankkarten-Größe, falls auch mobil genutzt, und eine passend große Klarsichtfolie. Nun bringt man diese in Deckung übereinander und markiert jeweils ein bestimmtes Randobjekt als Kalibrierung, also auf Blatt und Folie, z.B. mit einem Plus ⊕. Dies ist nötig, um die Nutzung zu vereinfachen. Nun überlegt man sich zu jedem Benutzerkonto ein starkes Passwort, z.B. Webshop 372++xy389, Telefonie 747&&19sUper usw. Es ist ok und gut, komplizierte Passwörter zu verwenden, da sie sicher aufgeschrieben und verwahrt werden. Diese notiert man mit Bleistift (da veränderbar) auf dem Blatt Papier (nur die Passwörter, sauber in Spalten und Zeilen getrennt) und ergänzt dabei eventuell - wie erfahrungsgemäß hilfreich - Hinweise wie "das ist Großbuchstabe", "Null" oder ähnliches, um Missverständnisse bestmöglichst auszuschließen. Nun schreibt man auf die kalibrierte,

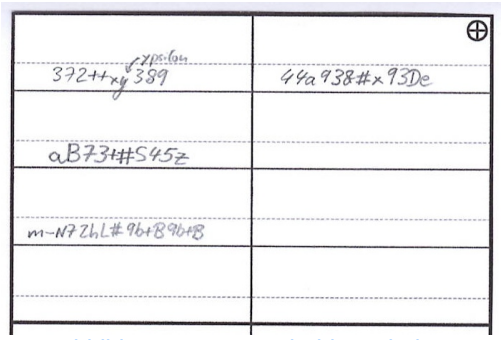

Abbildung 1: Das Papierblatt mit den Passwörtern in Zeilen und Spalten

Abbildung 2: Anwendung in kombinierter Version, Papierblatt und Folie aufeinander gelegt

also ausgerichtete Klarsichtfolie die zugehörigen Kennungen oder URLs o.ä. evtl. auch als Kombination mit dem Benutzernamen, also z.B. Mail Firma info@DresPleier.de. Dies mit einem unveränderlichen Folienschreiber oder anderen Stift, der versehentliches Löschen oder Ändern ausschließt. Das Ganze erfolgt so, daß übereinandergelegt beide Informationen lesbar sind, also jeweils die Dienstspezifikation auf der Klarsichtfolie oberhalb und darunter auf dem Papier das zugehörige Passwort. Damit hat man schon ein sehr gutes System bestehend aus zwei Teilen, Folie und Blatt, die nur zusammen und kombiniert einen Nutzen bringen.

Damit ist ein Schutz basierend auf dem Besitz zweier trennbarer Komponenten erreicht. Gelangen Folie und Papier in die Hände Unberechtigter, ist ein Missbrauch möglich. Einen zusätzlichen Schutz ergibt **Konzeptteil 5: Nutze neben Besitz auch Wissen, um Missbrauch durch Diebstahl zu verhindern**. Das bisherige Konzept wird gestärkt als 2-Faktor-Authentifikation als Besitz plus Wissen durch ein zusätzliches Geheimnis. Dieses merkt man sich und ergänzt es mit einem einheitlichen System, also z.B. immer vorne am Passwort als Konkatenation gemerktes, einheitliches Präfixpasswort konkateniert mit dem auf dem Blatt stehenden Passwort. Beispielsweise gemerkt 0815geheim++ zusammen mit dem Telefonie-Passwort ergibt 0815geheim++747&&19sUper.

Dies führt zu sehr starken Passwörtern (lang und komplex), die einfach zu ändern sind (mit Bleistift neu überschreiben) und bestmöglich vor Missbrauch geschützt sind (durch gemerktes Zusatz-passwort und die Trennung von Zuordnung Dienst bzw. Benutzername zu Passwort). Der Schutz hängt natürlich von der Wahl des gemerkten Passwortes ab (es sollte auch stark sein) und der geeigneten, getrennten Verwahrung von Folie und Blatt. Häufig benutzte Passwörter kann man

sich auch positionsmäßig merken, z.B. links oben steht das Webshop-Passwort, bei vielen Passwörtern wird dies aber dann nicht mehr ausreichen. Bei nur wenigen Diensten bzw. Passwörtern können die Leerplätze mit fingierten Diensten und Passwörtern als Zusatzschutz gegen Ausprobieren durch einen Angreifer gefüllt werden.

Nutzung

Die Sicherheit hängt neben geeigneter Kennungsnamen- und Passwörterwahl von der Trennung Folie und Blatt ab. Zuhause packt man eines der Objekte an einen besonders geschützten Ort (z.B. Tresor), das andere versteckt man an einem möglichst unauffälligen Platz (z.B. in einem Buch zwischen den Seiten). Wird der Tresor gestohlen oder zwangsgeöffnet, sind nicht beide Datenblätter "verloren". Auf Reisen verwendet man es ganz ähnlich: Ein Objekt trägt man immer bei sich oder bewahrt es besonders geschützt auf (typischerweise das Blatt, z.B. gefaltet im Geldbeutel oder im Hoteltresor); das andere Objekt (Folie) versteckt man ganz unauffällig, auch z.B. in einem Buch, das natürlich möglichst unattraktiv und für Angreifer (hier z.B. Diebe) uninteressant sein sollte (also z.B. kein aktuelles Männermagazin :-)). Die Wahrscheinlichkeit, daß beides abhanden kommt, ist sehr gering, da ein Angreifer den Hoteltresor ausräumen wird und das Buch vernachlässigt oder eben die Tasche mit dem Buch stiehlt und nicht den Tresor. Zusätzlich hat man noch das Geheimnis, also das Präfixpasswort im Kopf, das zum Missbrauch nötig wäre.

Ergänzend wichtig ist natürlich noch **Konzeptteil 6: Halte bei Verlust geeignet Passwort-Reset-Prozesse oder eine (nicht-digitale) Sicherheitskopie der Passwörter an einem sicheren Ort vor**. Dies aber eben nicht als Kopie mit einem an das Netzwerk angeschlossenen Kopierer oder gescannt o.ä.; alles, was digital vernetzt ist oder speichert, ist für Backups ausgeschlossen (Kopierer, Scanner, Smartphone- oder Kamera-Fotos mit drahtloser Verbindung oder Netz-/Cloud-Speicher usw.). Einfach und pragmatisch ist eine Kopie der einzelnen Teile (Folie und Blatt) mittels einem Offline-Kopierer.

Zur Nutzung gilt **Konzeptteil 7: Die Passwörter werden dauerhaft offline gehalten und verwendet, d.h. eingetippt, wobei auf einen geeigneten Schutz bei der Verwendung vor Abschauen, Aufzeichnen, Fotografieren usw. zu achten ist**. Dazu die Passwörter nirgends in Anwendungen zwischenspeichern und die Passwort-Tabelle nicht vor Kameras anwenden wie Smartphone-, Laptop- oder Überwachungskameras o.ä. oder anderen Personen, die diese abschauen können. Die Passwort-Tabelle, die Tastatur bzw. das Eintippen dazu abdecken oder aus dem Sicht-/Aufnahmebereich entfernen (z.B. unter dem Schreibtisch, unter einer Jacke, Dazwischenstellen usw.).

ABCD	EFGH	IJKL	MNOP	QRST	UVWX	YZ.-/	0123	456	789
2hL#	4g&M	9b+B	m-N7	W#2w	+r0A	G8k+	aB3*	1*De	S5+y

Abbildung 3: Eine Passwort-Generator-Tabelle

Zusatzsicherheit

Sofern Jemand in der Lage ist, selbst starke Passwörter zu wählen (lang, komplex, keine persönlichen Daten usw.), werden diese direkt bestimmt und ist eine zusätzliche Passwort-Generator-Tabelle ohne erkennbaren Mehrwert. Ansonsten ist diese ergänzend eine gute Option als **Konzeptergänzung 1: Nutze bei Bedarf eine Passwort-Generator-Tabelle zum Erzeugen starker Passwörter**. Diese kann auf dem Zettel mit aufgebracht und mit einem bestimmten System benutzt werden, indem man z.B. die ersten 5 Buchstaben von der URL der Dienstadresse oder des Dienstnamens (Telefonie oder Mailprivat oder Maildienstlich) nimmt. Eine Generator-Tabelle enthält eine Zuordnung von Buchstaben und Ziffern zu Passwortteilwörtern, die für starke Passwörter eine Kombination aus Buchstaben, Ziffern und Sonderzeichen sind, sowie Groß- und Kleinschreibung beachten. Durch Einsatz einer solchen Tabelle können schwache Passwörter methodisch vermieden werden. Beispielsweise ergibt die Tabelle in Abbildung 3 bei Mailprivat m-N72hL#9b+B9b+Bm-N7.

Möchte man die Lösung weiter verbessern, kann man auf der Folie mit einer Farbe arbeiten, die nur mittels UV-Lampe sichtbar wird und damit die Folie "tarnen" als "wertlos" oder sogar mit anderen Dingen zwischen den Zeilen beschreiben, um die Folien- bzw. Passwörterbedeutung zu verstecken. Zum Anwenden benötigt man dann aber eine UV-Lampe, um die Zeichen sichtbar zu machen; dies wäre **Konzeptergänzung 2: Tarne die Folieninformationen gezielt durch Nutzung unsichtbarer Farbe und optionalen Aufbringen lesbarer unscheinbarer Informationen**.

Praxistipps

In der Anwendung haben wir gute Erfahrungen gemacht für die mobile Nutzung in der Größe einer doppelten Bankkarte, die in der Mitte gefaltet wird und dann in einer (RFID-) Schutzhülle für Bankkarten geschützt und gegebenenfalls hinter einer echten Karte verborgen aufbewahrt wird. Der Folienstift sollte fein schreibbar und auch wirklich permanent sein, um ein versehentliches Verwischen oder Löschen zu verhindern, was in der Praxis durchaus vorkam; ein zeilenweises Aufbringen eines durchsichtigen Klebebands über der Folienschrift ist hier ein pragmatischer Zusatzschutz. Die Folie als "Folientasche", aus z.B. Klarsichthülle hergestellt, vereinfacht die Verwendung deutlich, da damit das Kalibrieren beschleunigt und ein Verrutschen von Folie zu Papier verhindert wird. Für den getarnten Einsatz sind keine "Geheimstifte", sondern professionelle "UV Permanent Marker" zu empfehlen, um auch Kunststoff beschreiben zu können; der Schutz wird erhöht, da normalerweise bzw. geeignetes Medium gewählt oder getarnt die Schrift nicht erkennbar bzw. unauffällig ist; für einen mobilen Einsatz ist eine Schwarzlicht-Taschenlampe nötig; trotz Einsatz der Lampe war keine Backup-Kopie via Kopierer möglich, via Foto schon. Ein Vorlage Muster wie in Abbildung 4 ist hilfreich, um die Zeilen und Spalten besser zu nutzen.

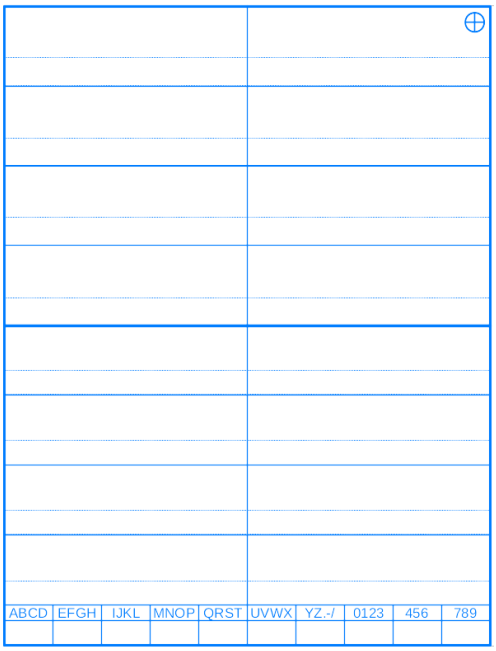

Abbildung 4: Das Muster für das Papierblatt mit Kalibrierungssymbol, Zeilen und Spalten sowie vorbereiteter Passwort-Generator-Tabelle (siehe www.DresPleier.de)

Fazit

Das Konzept hat alles, was nötig ist: starke Passwörter, über Kodierungstabelle sogar generierbar; dynamische, veränderliche Passwörter; 2-Faktor-Authentifikation, besser sogar als 2,5-Faktor-Authentifikation, da 2x Besitz und 1x Wissen nötig ist; geeignete Aufbewahrung; mobil nutzbar; Backup-Konzept; steganographische Tarnmöglichkeit. Zudem enthält es implizit eine Synchronisierung über Geräte-/Systemgrenzen hinweg, da der Sichere-Passwort-Speicher als zentrales Datenmedium verwendet wird. Es ist eine sehr gute Lösung, die individuell ausgeprägt werden kann. Man kann z.B. unterschiedliche Farben verwenden, um Passwörter zu markieren (auf dem Bleistiftblatt), also z.B. ein roter Punkt beim Administrator- oder ein blauer bei seinem Mail-Konto; man kann die Verstecke individuell auswählen, entsprechend seiner persönlichen Nutzungsperspektive; man kann die Folientarnung unterschiedlichst gestalten, z.B. eine Filmhülle aus seiner umfangreichen Filmsammlung oder eine Klarsichtfolie in seiner Arbeitsmappe einsetzen; und man kann sogar ein 4-Augen-Prinzip realisieren: eine Person hat die Folie, eine andere den Passwortzettel, beide müssen zusammenarbeiten. Die von der DresPleier GmbH entwickelte neuartige Lösung DresPleierPwS ist "rund", einfach, sehr pragmatisch, individuell ausprägbar und sehr sicher für die nicht-digitale Speicherung und Verwendung von Passwörtern. DresPleierPwS ist eine Erfindung und Wertschöpfung der DresPleier GmbH und ist für die rein private Nutzung kostenlos nutzbar, alle anderen Nutzungen (in Firmen, Vereinen, Verbänden, Behörden usw.) sind zu lizenzieren.

Firma: DresPleier GmbH ; **Geschäftsführer:** Dr. Christoph Pleier ; **Sitz und Registergericht:** Landshut HRB 6587 ; **USt-ID:** DE814347435
Anschrift: Vils 8, 84149 Velden ; **Telefon:** 08742/5870894 ; **Telefax:** 03222/4170655 ; **Mail:** info@DresPleier.de ; **Web:** www.DresPleier.de