Notfallzettel: Passwortmanager

Vergessen, verloren, kompromittiert · gehört zu Kapitel 18 und 13 · Manager: [ ] KeePassXC [ ] Proton Pass · Stand der Vorsorge: _____

Der Passwortmanager ist der Generalschlüssel. Genau deshalb ist das Klumpenrisiko ernst zu nehmen: Fällt er aus, hängen alle Konten daran. Ein Manager fällt aber selten durch Hacker aus, sondern durch drei Alltagsfälle: die Master-Passphrase ist vergessen, die Datei oder das Gerät ist weg, der zweite Faktor ist verloren. Gegen alle drei hilft nur Vorsorge, die vor dem Ernstfall erledigt ist. Dieser Zettel sortiert beides, die Vorsorge oben und den Ernstfall unten. Er trägt aber nur, wenn Teil A vorher abgehakt ist. Die eigentliche Master-Passphrase steht nie auf diesem Blatt, sondern handschriftlich auf dem separaten Notfallblatt im versiegelten Umschlag des Disaster Kits (Kapitel 13).

A · VORHER, DAMIT DER ZETTEL IM ERNSTFALL TRÄGT

Punkt	OK	Notiz
Die Master-Passphrase besteht aus sechs oder mehr zufälligen Wörtern aus der EFF-Liste, gewürfelt oder vom Generator erzeugt. Sie existiert nur im Kopf und einmal handschriftlich auf dem Notfallblatt im Disaster Kit (Kapitel 18, Regel 2 und 3). Hier nur das Kürzel des Ortes.		Notfallblatt bei: _____
Im Browser ist kein Passwort mehr gespeichert. Alles wurde in den Manager übernommen und der Browser-Speicher geleert. Der Browser ist die Angriffsfläche, nicht der Tresor.		
Der Manager wurde einmal von einem zweiten Gerät aus geöffnet (Rechner, Zweitgerät oder Smartphone). Sonst fehlt im Ernstfall der Schlüssel zu allem anderen.		Zweitgerät: _____
KeePassXC: Die KDBX-Datei liegt in der 3-2-1-Sicherung (drei Kopien, zwei Medien, eine außer Haus), die Kopie außer Haus verschlüsselt, bevor sie das Haus verlässt (Kapitel 13).		Letzte Sicherung: _____
KeePassXC: Schlüsseldatei und Hardware-Token sind gesichert. Die Schlüsseldatei liegt getrennt von der Datenbank, der Hardware-Token (YubiKey) hat einen Ersatz-Token, der mit demselben Geheimnis programmiert wurde, oder das Geheimnis liegt auf Papier im Disaster Kit. Ohne Schlüsseldatei oder Token bleibt die Datenbank auch mit Passphrase verschlossen.		Schlüsseldatei bei: _____
Proton Pass: Der Wiederherstellungssatz des Proton-Kontos ist erzeugt und liegt auf Papier im Disaster Kit. Nur er stellt Passwort und Daten zugleich wieder her. Eine Wiederherstellungs-E-Mail allein setzt nur das Passwort zurück, die Einträge bleiben verschlüsselt. Das Proton-Konto selbst hat einen zweiten Faktor. Ein verschlüsselter Export der Einträge liegt als Offline-Kopie in der Sicherung.		Wiederherstellung bei: _____
Die Recovery-Codes der wichtigsten Konten liegen ausgedruckt im Disaster Kit: Haupt-E-Mail zuerst, dann Bank, Proton, Nostr-Schlüssel-Backup. Wo ein Hardware-Schlüssel den zweiten Faktor stellt, ist ein Ersatzschlüssel registriert (Kapitel 18, Regel 7).		Ersatzschlüssel bei: _____
Der Restore-Test ist gelaufen: Die Sicherung wurde einmal nach der Einrichtung und danach jährlich auf einem anderen Gerät geöffnet. Ein Backup, das nie zurückgespielt wurde, ist nur eine Hoffnung.		Letzter Test: _____
Angehörige wissen, dass es das Disaster Kit gibt und wo das Notfallblatt liegt. Für die Kopie im Bankschließfach haben sie eine Bankvollmacht (Kapitel 13).		Eingeweiht: _____

B · IM ERNSTFALL

Nr	Fall und Schritte	Warum	Erledigt
1	**Master-Passphrase vergessen.** KeePassXC: Es gibt keinen Reset. Der einzige Weg ist das handschriftliche Notfallblatt im Disaster Kit. Proton Pass: das Passwort über den Wiederherstellungssatz aus dem Disaster Kit zurücksetzen. Danach eine neue Passphrase setzen und das Notfallblatt erneuern.	Die Verschlüsselung kennt keine Hintertür, auch nicht für dich. Ohne Notfallblatt ist die Datenbank endgültig verloren.	
2	**Datei beschädigt oder Gerät weg.** KeePassXC: die Sicherung aus dem 3-2-1-Backup holen, dazu Schlüsseldatei und Token, auf dem Zweitgerät öffnen. Proton Pass: auf dem Zweitgerät anmelden, das verlorene Gerät aus den aktiven Sitzungen des Kontos abmelden.	Die Sicherung ist der einzige Weg zurück zu den Daten. Eine offene Sitzung auf einem fremden Gerät bleibt sonst ein Zugang.	
3	**Zweiter Faktor verloren.** Mit den Recovery-Codes aus dem Disaster Kit oder dem Ersatz-Hardwareschlüssel anmelden. Danach einen neuen Faktor registrieren, den alten entfernen und die verbrauchten Codes durch neue ersetzen.	Ein zweiter Faktor sperrt im Zweifel auch dich selbst aus. Verbrauchte Codes sind kein Sicherheitsnetz mehr.	
4	**Verdacht auf Kompromittierung** (Malware, Datenleck, fremde Sitzung). Von einem sauberen Gerät aus zuerst die Master-Passphrase ändern, dann die Passwörter in dieser Reihenfolge: Haupt-E-Mail, Bank, Proton, danach alles andere. Alle Sitzungen abmelden, die eigenen Adressen bei haveibeenpwned prüfen, Zweitfaktor-Token erneuern.	Über die Haupt-E-Mail lassen sich fast alle anderen Passwörter zurücksetzen. Wer die Reihenfolge einhält, schließt die Tür, bevor der Angreifer sie nutzt.	
5	**Dauerhafter Ausfall** (Unfall, Tod). Angehörige öffnen das Disaster Kit: Notfallblatt, Anleitung und Vollmacht liegen dort zusammen (Kapitel 13, digitaler Nachlass).	Kein Gericht öffnet verschlüsselte Daten. Was nicht dokumentiert ist, ist für die Erben verloren.	

Datenbank-Sicherung liegt bei (Kürzel): _____ · Notfallblatt liegt bei (Kürzel): _____ · Zweitgerät: _____ · Ersatz-Token liegt bei (Kürzel): _____

⚠ **Keine Passphrase, kein Recovery-Code, kein Kontoname auf diesen Zettel**, auch nicht „zur Sicherheit". Orte nur als Kürzel, die nur du deuten kannst (Beispiel „T2" für Tresorfach 2, „OM" für den Ordner bei einem Angehörigen). ⚠ **Das handschriftliche Notfallblatt mit der Passphrase ist das einzige Dokument, das den Manager öffnet.** Es gehört in den versiegelten Umschlag, nirgendwo sonst, nie digital.