Das Datenleck Collection #1 - #5

FH-Prof. Dr. Harald Lampesberger
Department Sichere Informationssysteme

HAGENBERG | LINZ | STEYR | WELS

FH OBERÖSTERREICH
UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA

Für „DIGITAL VERNETZT & AUSSPIONIERT! 2019“ zugelassen.

Am 17. Jänner 2019

Zum Download in einem öffentlichen Hacking-Forum

- Collection #1 87,18GB
- Collection #2 526,11GB
- Collection #3 37,18GB
- Collection #4 178,58GB
- Collection #5 42,79GB
- ANTIPUBLIC #1 102,04 GB
- AP MYR&ZABUGOR #2 24,53GB

Ziele für heute

Wer ist betroffen?

Welches Problem ergibt sich daraus?

Wie kann man sich schützen?

Ein paar Eckdaten

937 GB Daten

- Primär Email-Adressen, Passwörter
- Aber auch Benutzernamen, Telefonnummern

2,7 Milliarden Einträge

- 1,2 Milliarden Email-Passwort-Kombinationen
- 773 Mio. Emailadressen
- 21 Mio. einzigartige Klartextpasswörter

Weltweit User betroffen

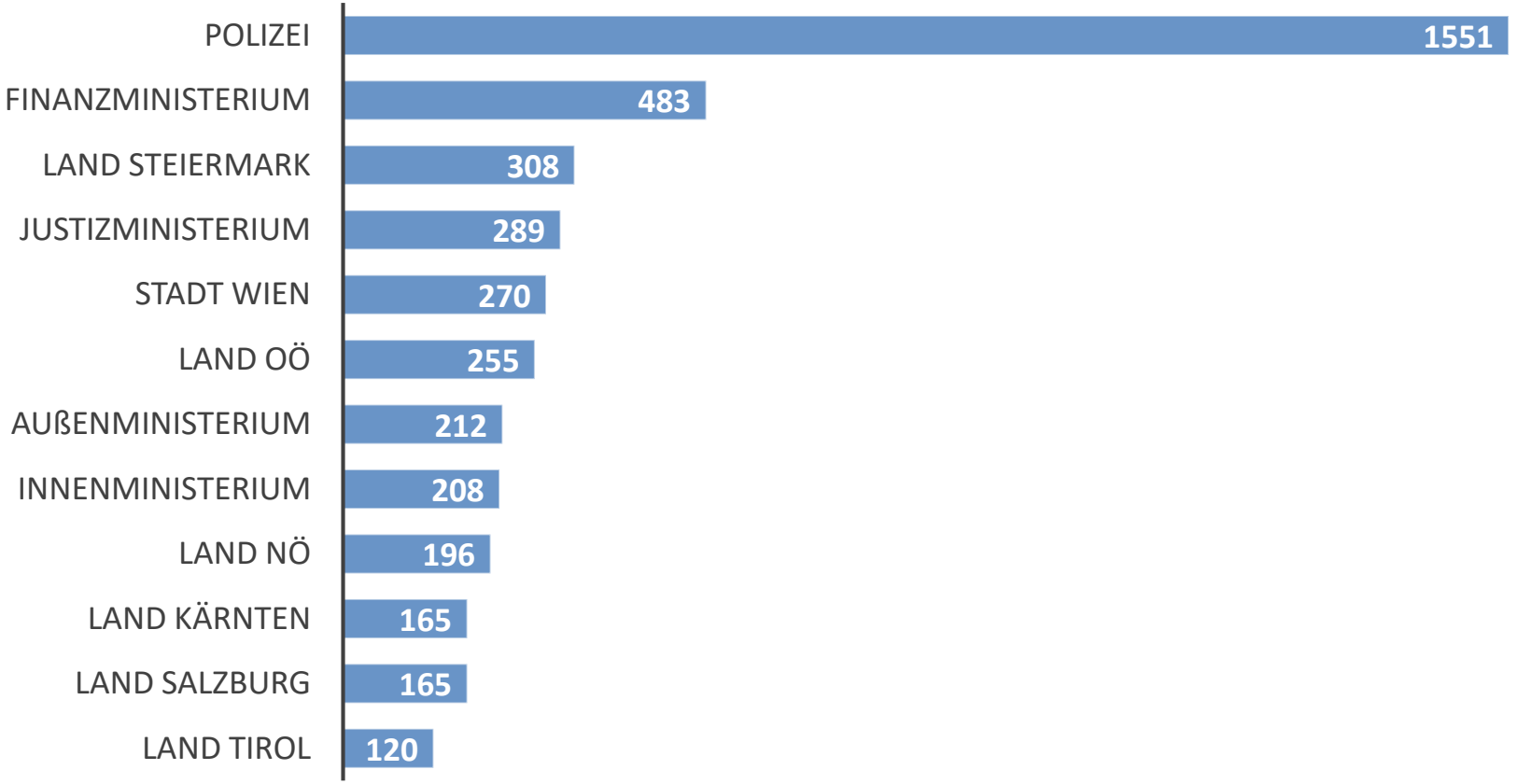
- Viele frühere Datenlecks
- Herkunft eines Eintrags in den meisten Fällen nicht nachvollziehbar

```
Collection  #1_NEW combo semi private_Dumps
Collection  #1_NEW combo semi private_EU combo
Collection  #1_NEW combo semi private_Private combos
Collection  #1_NEW combo semi private_Update Dumps
Collection  #1_Number pass combos
Collection  #1_OLD CLOUD_BTC combos
Collection  #1_OLD CLOUD_CHINA combos
Collection  #1_OLD CLOUD_Dump cleaned - deleted duplicated and trash
Collection  #1_OLD CLOUD_Gaming combos
Collection  #1_OLD CLOUD_Hacking combos
Collection  #1_OLD CLOUD_Japan combos
Collection  #1_OLD CLOUD_Monetary combos
Collection  #1_OLD CLOUD_OLD DUMPS DEHASHED
Collection  #1_OLD CLOUD_Porn combos
Collection  #1_OLD CLOUD_Shopping combos
Collection  #1_OLD CLOUD_Trading combos
Collection  #1_OLD CLOUD_UK combos
Collection  #1_OLD CLOUD_USA combos
Collection  #1_RU combo
Collection  #1_Shopping combos
Collection  #1_USA combos
Collection  #1_USER PASS combos
Collection #2_New combo cloud_Database Collection_Dump расшифрованные
```

123456

ist noch immer das häufigste Passwort.

Österreichische Politik betroffen



Quelle: SRF Data / Addendum https://www.addendum.org/politometer/kategorie/gesetzgebung/politiker-passwoerter/

Rechnen Sie damit, dass Ihre Passwörter irgendwann im Klartext auftauchen.

Identitätsdiebstahl

Problem: Gleiches Passwort für viele Dienste

Email-Account ist kritisch

- Ungewollte Bestellungen
- Zahlungsgeschäfte / PayPal / Crypto
- Betrugskriminalität
- Erpressung
- …

Wie kann man sich schützen?

Schritt 1: Email-Adresse prüfen

Hasso-Plattner-Institut https://sec.hpi.de/ilc/

Result of Your Request for the HPI Identity Leak Checker

Attention: Your e-mail address appears in at least one stolen and illegally published identity data base (a so-called identity leak).
The following sensitive information was freely found on the Internet in connection with your e-mail address:

Affected Service	Date	Verified	Affected users	Password	First and last name	Date of birth	Address	Telephone number	Credit card	Bank account details	Social security number	IP Address
Unknown (Collection #1-#5)	Jan. 2019		2,191,498,885	Affected	–	–	–	–	–	–	–	–
	This dataset was published in January 2019 and contains huge lists of credentials of unknown origin, older leaks and smaller database dumps.											
dropbox.com	Sep. 2012	✓	68,658,165	Affected	–	–	–	–	–	–	–	–

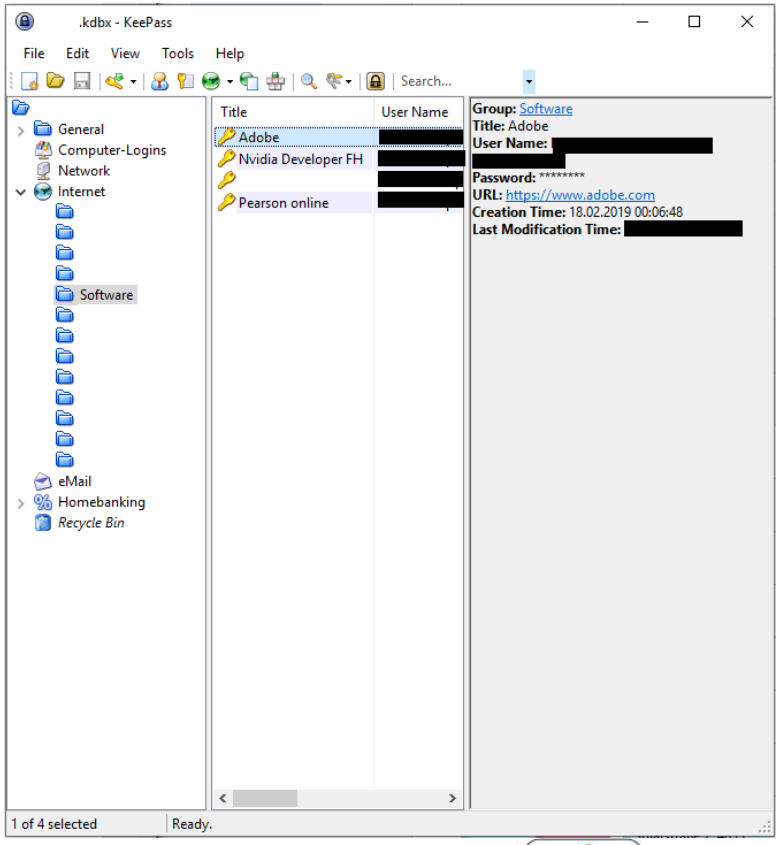
Schritt 2: Gute Passwörter

Tipp: Einzigartige Passwörter

- Begrenzt Schaden
- Rückverfolgbar

Tipp: Passwortmanager

- zB Keepass2
- Open Source
- Verschlüsselte Datenbank
- Passwortgenerator



Übrigens: Passwortrichtlinien

Sie kennen das sicher …

- „Ihr Kennwort läuft in 2 Tagen ab“
- „Verwenden Sie ein Sonderzeichen, eine Ziffer und einen Großbuchstaben“

Neuer Stand der Technik: NIST SP 800-63B

- Mindestens 8 Zeichen lang (besser 12) und mehr als 64 Zeichen erlaubt
- Keine Komplexitätsvorgaben, alle Zeichen erlaubt
- Passwort darf nicht in einem Datenleck vorkommen
- Keine Erinnerungstipps
- Kein regelmäßiger Wechsel, nur anlassbezogen

Schritt 3: Multifaktor-Authentisierung

Bei kritischen Diensten

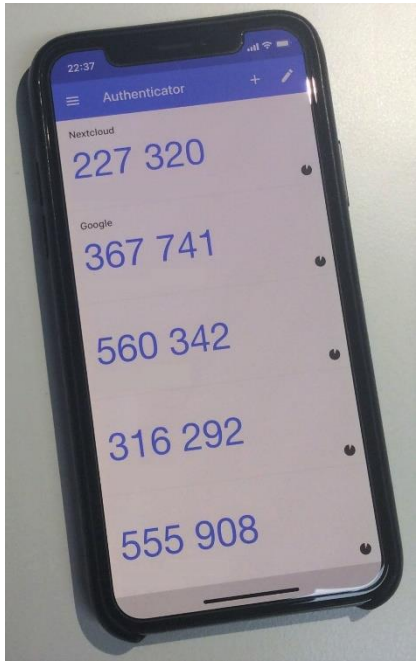
- Email-Account, Online-Banking, Cloud-Dienste

Tipp: Google Authenticator

- Generiert Einmal-Passwörter
- Breite Unterstützung, zB Nextcloud

Tipp: Yubico Security Key

- Günstiger USB-Token
- Unterstützt in allen aktuellen Browsern
- Funktioniert sofort mit vielen Web-Diensten



Zusammenfassung

Datenlecks werden passieren

- Immer damit rechnen, dass Passwörter öffentlich werden
- Einzigartige starke Passwörter verwenden
- Passwortmanager
- Multifaktor-Authentisierung

Diensteanbieter

- Passwörter nie im Klartext speichern
- Multifaktor-Authentisierung integrieren
- NIST SP 800-63B